REMARKS

Applicants cancel claim 2. Claims 1 and 3-28 remaining pending in the application. Applicants amend claims 1 and 4-6 to incorporate features of claim 2 and for further clarification. No new matter has been added.

Claims 1-8, 10-15, 17-19, 21-25, 27-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,818,936 to Mashayekhi in view of U.S. Patent No. 5,761,309 to Ohashi et al.; and claims 9, 16, 20, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,818,936 to Mashayekhi in view of U.S. Patent No. 5,761,309 to Ohashi et al., further in view of U.S. Patent No. 5,892,828 to Perlman. Applicants amend claims 1 and 4-6 to incorporate features of claim 2 and to further clarify the invention as distinguished from the cited references. Applicants respectfully traverse the rejection.

The Examiner maintained the rejections by arguing that the public key scheme described in Mashayekhi includes a private key used by a sender to sign information so that a recipient may authenticate the sender of the information. Page 11, lines 6-12 of the Office Action. The Examiner, therefore, apparently applied the public/private key pair described in Mashayekhi as alleged disclosure of the claimed issuance side processed value.

Applicants respectfully submit that the described public/private key pair fails to disclose this feature. Mashayekhi, as cited and relied upon by the Examiner, only describes a certification authority cryptographically binding a public key and a user name in a signed "certificate," and choosing the public/private key pairs at random. As such, Mashayekhi does not disclose or

suggest generating either the public or private key "by encrypting the information of the original group information."

Mashayekhi describes,

> "the KG must choose private/public key pairs at random ... [and] the KG must reliably communicate the generated public key to certification authority 220, so that the CA (e.g., another specialized server application) may cryptographically bind the public key and the user name in a signed 'certificate'." Col. 5, lines 46-54 of Mashayekhi. (Emphasis added)

Therefore, Mashayekhi, as cited and relied upon by the Examiner, merely describes a certification authority 220 that "cryptographically bind[s] [a] public key and [a] user name" to obtain a signed "certificate." Mashayekhi, therefore, fails to disclose a "group certificate issuing apparatus" that issues a group certificate based on "original group information including the name of the group to which the related user belongs," as claimed. (Emphasis added) Mashayekhi only describes choosing a private/public key pair at random. Therefore, the key pair does not include any information on a user or the group to which the user belongs. Applicants respectfully submit that the certificate described in Mashayekhi, thus, fails to meet the claimed features related to a "group certificate."

Correspondingly, Mashayekhi, as cited and relied upon by the Examiner, also fails to disclose adding to the original group information an issuance side processed value that is "obtained by encrypting the information of the original group information by a cryptographic function," as claimed.

Furthermore, Mashayekhi, as cited and relied upon by the Examiner, does not disclose first and second secret information assigned to a group kept, respectively, at the group certificate

issuing apparatus and group certificate verification unit for group information and information in a received group certificate.

In other words, Mashayekhi, as cited and relied upon by the Examiner, fails to disclose or suggest,

> "[a] system of distributed group management for indirectly authenticating membership of a user in a group in order to manage security for a client on a client side and a server for executing a remote processing request from the client side under a predetermined authorization assigned for every group, provided with
>
> a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs when there is said remote processing request and
>
> a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server, wherein
>
> said group certificate issuing apparatus adds an issuance side processed value obtained by encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate,
>
> said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide,
>
> said group certificate issuing apparatus includes first secret information assigned to said groups in said original group information and performs the processing by said cryptographic function, said first secret information being held only by said group certificate issuing apparatus,
>
> said group certificate verification unit includes second secret information assigned to the groups in part of information included in said received group certificate and performs the processing by said cryptographic function, said second secret information being held only by said group certificate verification unit, and

said first secret information and said second secret information are identical secret information for identical groups," as recited in claim 1. (Emphasis added)

The Examiner relied upon Ohashi et al. as a combining reference to specifically address the claimed feature of performing an "authentication by confirming that said issuance side processed value and said verification side processed value coincide." Page 4, lines 15-21 of the Office Action. Therefore, even assuming, arguendo, that it would have been obvious to one skilled in the art to combine Mashayekhi and Ohashi et al., the combination would still have failed to disclose or suggest the above-cited features of claim 1.

Accordingly, Applicants respectfully submit that claim 1, together with claim 3 dependent therefrom, is patentable over Mashayekhi and Ohashi et al., separately and in combination, for at least the above-stated reasons. Claims 4-6 incorporate features that correspond to those of claim 1 cited above, and are, therefore, together with claims 7-8, 10-15, 17-19, 21-25, 27-28 dependent therefrom, respectively, patentable over the cited references for at least the same reasons.

The Examiner relied upon Perlman to specifically address the additional features recited in dependent claims 9, 16, 20, and 26. As such, the combination of this reference, even if obvious to one skilled in the art at the time the claimed invention was made, would still have failed to cure the above-described deficiencies of Mashayekhi and Ohashi et al. Accordingly, Applicants respectfully submit that claims 9, 16, 20, and 26 are patentable over the cited references for at least the above-stated reasons with regard to their respective base claims 5 and 6, from which they depend.

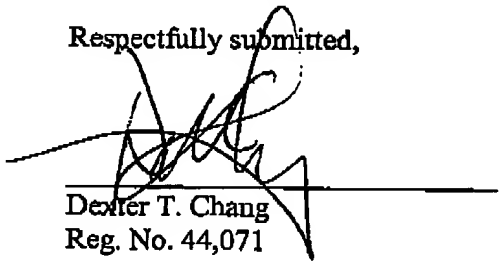
The above statements on the disclosure in the cited references represent the present opinions of the undersigned attorney. The Examiner is respectfully requested to specifically indicate those portions of the respective reference that provide the basis for a view contrary to any of the above-stated opinions.

Applicants appreciate the Examiner's implicit finding that the additional reference made of record, but not applied, does not render the claims of the present application unpatentable, whether this reference is considered alone or in combination with others.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,



Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11702 (FUJA 18.671)
DTC:bf

84121930_1.DOC
NYC01_84121930_1_100794_11702